REMARKS

Claims 1 – 4, 6, 8 – 16, 18 and 20 - 28 are pending in the present application. Claims 5, 7, 17, 19 and 29 were previously canceled.

On page 3 of the Office Action, claims 1 – 4, 8 – 16 and 20 – 28 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,886,038 to Tabbara et al. (hereinafter "the Tabbara et al. patent"). From page 4 of the Office Action, it is apparent that the Examiner intended to also reject claim 18, and so, Applicant is treating this rejection as a rejection of claims 1 – 4, 6, 8 – 16, 18, and 20 – 28. Nevertheless, Applicant is traversing this rejection.

Claim 1 recites a method for providing a switch user (SU) functionality in a server-agent environment. The method includes, *inter alia*, signing an SU certificate with a signature using a private key, and authenticating the signature with a public key.

The Office Action contends that the Tabbara et al. patent, in a passage at col. 14, lines 50 – 64, discloses signing an SU certificate with a signature using a private key. The passage at col. 14, lines 50 – 64 states:

> Having a public/private key pair in which BMonitor 250 stores the private key and the tenant knows the public key allows information to be securely communicated from the tenant to BMonitor 250. In order to ensure that information can be securely communicated from BMonitor 250 to the tenant, an additional public/private key pair is generated by the tenant and the public key portion is communicated to BMonitor 250. Any communications from BMonitor 250 to the tenant can thus be encrypted using this public key portion, and can be decrypted only by the holder of the corresponding private key (that is, only by the tenant). (emphasis added)
>
> BMonitor 250 also maintains, as one of keys 259, a disk key which is generated based on one or more symmetric keys (symmetric keys refer to secret keys used in secret key cryptography).

Thus, the Tabbara et al. patent expressly describes encrypting using a public key, rather than signing an SU certificate with a signature using a **private key**, as recited in claim 1.

Additionally, the Office Action contends that the Tabbara et al. patent, in a passage at col. 17, lines 14 – 39, discloses authenticating the signature with a public key. The passage at col. 17, lines 14 – 39 states:

> BMonitor 250 authenticates a management device(s) corresponding to each of the ownership domains. BMonitor does not accept any commands from a management device until it is authenticated, and only reveals confidential information (e.g., encryption keys) for a particular ownership domain to a management device(s) that can authenticate itself as corresponding to that ownership domain. This authentication process can occur multiple times during operation of the node, allowing the management devices for one or more ownership domains to change over time. The authentication of management devices can occur in a variety of different manners. In one implementation, when a management device request a connection to BMonitor 250 and asserts that it corresponds to a particular ownership domain, BMonitor 250 generates a token (e.g., a random number), encrypts the token with the public key of the ownership domain, and then sends the encrypted token to the requesting management device. Upon receipt of the encrypted token, the management device decrypts the token using its private key, and then returns the decrypted token to BMonitor 250. If the returned token matches the token that BMonitor 250 generated, then the authenticity of the management device is verified (because only the management device with the corresponding private key would be able to decrypt the token). An analogous process can be used for BMonitor 250 to authenticate itself to the management device. (emphasis added)

Thus, the Tabbara et al. patent expressly describes decrypting using a private key, rather than authenticating the signature with a **public key**, as recited in claim 1.

In summary:

(a) the Tabbara et al. patent describes encrypting using a public key, whereas claim 1 recites signing an SU certificate with a signature using a **private key**; and

(b the Tabbara et al. patent describes decrypting using a private key, whereas claim 1 recites authenticating the signature with a **public key**.

Thus, with regard to the use of a public key and a private key, the Tabbara et al. patent describes a method that is opposite of the method of claim 1. Hence, the Tabbara et al. patent does not anticipate claim 1.

Claims 13 and 25 each include recitals similar to those of claim 1, as described above. As such, claims 13 and 25, for reasoning similar to that provided in support of claim 1, are also novel over the Tabbara et al. patent.

Claims 2 – 4, 6, and 8 – 12 depend from claim 1; claims 14 – 16, 18 and 20 – 24 depend from claim 13; and claims 26 – 28 depend from claim 25. By virtue of these dependencies, claims 2 – 4, 6, 8 –12, 14 – 16, 18, 20 – 24 and 26 – 28 are also novel over the Tabbara et al. patent.

Applicant respectfully requests reconsideration and withdrawal of the section 102(e) rejection of claims 1 – 4, 6, 8 – 16, 18, and 20 – 28.

In view of the foregoing, Applicant respectfully submits that all claims presented in this application patentably distinguish over the prior art. Accordingly, Applicant respectfully requests favorable consideration and that this application be passed to allowance.

Respectfully submitted,

1 AUG 2006
Date

John Yankovich
Reg. No. 42,240
Attorney for the Applicant
Ohlandt, Greeley, Ruggiero & Perle, L.L.P.
One Landmark Square, 10th Floor
Stamford, CT 06901-2682
Tel: 203-327-4500
Fax: 203-327-6401